Red Hall Primary School

E-Safety Policy

Document History	
Originally Written:	January 2017
Updated:	Sept 2024
By:	Ryan Todd
Additional guidance added:	
Approved by Governing Body:	*23/03/2022*
	21st October, 2024
Next Review Date:	October, 2025

This policy needs to read in conjunction with the Virtual Learning Policy.

Introduction

Our E-Safety Policy has been discussed with the school council, staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Context and Background

IT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

• The Internet – World Wide Web
• e-mail
• Instant messaging (often using simple web cams) e.g. Instant Messenger)
• Web based voice and video calling (e.g. Skype)
• Online chat rooms
• Online discussion forums
• Social networking sites (e.g. Facebook)
• Blogs and Micro-blogs (e.g. X)
• Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
• Video broadcasting sites (e.g. You Tube)
• Music and video downloading (e.g. iTunes)
• Mobile phones with camera and video functionality
• Smart phones with e-mail, messaging and internet access
- Online gaming (e.g. X – box, PS4)
- Apps (e.g. WhatsApp, Snapchat)

Our whole school approach to the safe use of IT

Creating a safe IT learning environment includes three main elements at this school:

• An effective range of technological tools;
• Policies and procedures, with clear roles and responsibilities
• E-Safety teaching is embedded into the school curriculum and schemes of work in all year groups

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Leadership team
The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures

E - afety Co-ordinator
Our school E-Safety Co-ordinators are Ryan Todd (Lead of Computing) and Carly Egglestone (Lead of PSHE). They are responsible for keeping up to date on all E-Safety issues and ensuring that staff are updated as necessary.

Governors
The School Governing body is responsible for overseeing and reviewing all school policies, including the E-Safety Policy.

School Staff
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school E-Safety policy, and ask for clarification where needed. They should sign the Staff Acceptable Internet Use agreement annually. Class teachers should ensure that pupils are aware of the E-Safety rules, introducing them at the beginning of each new school year and reinforcing throughout. Staff also need to reinforce the virtual learning home agreement with pupils.

Pupils
Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with E-Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using
IT at school and home.

Parents
Parents are to be given information about the school's E-Safety policy when requested. The E-Safety policy is displayed on the school's website. Any recent updates about current concerns (regarding games, apps and other online sources) are disseminated to parents and carers via our school website, parent mail and our Facebook page.

Technical and hardware guidance

School Internet provision
The school uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

• All pupils and staff have been issued with clear guidelines on what to do if this happens, and parent will be informed where necessary.
• Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading files and applications
The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

• Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

Portable storage media

• G drive must be used rather than a portable storage device, to abide by GDPR guidelines. All staff will receive support and training in using this efficiently.

Security and virus protection

The school subscribes to antivirus software. The software is monitored and updated regularly by the IT Administrator.
• Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the IT Administrator.

E-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and IT is an integral part of that world. At our school we are committed to teaching pupils to use the IT effectively and appropriately in all aspects of their education.

Internet access at school

Use of the Internet by pupils
Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

Access for all pupils
In line with inclusion policies across the school, we want to ensure that all out pupils have access to the Internet, particularly where this will directly support their learning. To this end, we provide lunchtime access and support for pupils at "Lunchtime drop in" sessions.

Using the Internet for learning
The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum for researching information, a source of digital learning materials and to deliver lessons. Using the Internet for learning is now a part of the school's Computing Curriculum (Sept 2016). We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

• Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
• Children are taught how to use search engines and how to evaluate Internet-based information as part of the IT curriculum, and in other curriculum areas where necessary.
• They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
• They are taught how to carry out simple checks for bias and misinformation.
• They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Teaching safe use of the Internet and IT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area. Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES. http://www.kidsmart.org.uk. We also use Google Internet Legends.

The main aspects of this approach include the following five SMART tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...

Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...

Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...

Tell your parent or carer if someone or something makes you feel uncomfortable or worried..

Suitable material
We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Unsuitable material
Despite the best efforts of school staff, and filtering software in place, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing the IT Administrator.
3. Logging the incident on the Google shared drive.
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

Using E-Mail at school
E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.
• We teach the use of e-mail as part of our IT curriculum, and use appropriate pupil email accounts.
• Pupils are not allowed to access personal e-mail using school Internet facilities.
- Pupils are not allowed to contact one another by email and can only contact staff through the class email address.

Chat, discussion and social networking sites
These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media. We teach children how to use chat rooms safely and actions to take if they do not feel safe.

Internet-enabled mobile phones and handheld devices
More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog. Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.
• Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

Cyberbullying - Online bullying and harassment
Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:
• No access to public chat-rooms, Instant Messaging services and bulletin boards.
• Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.
• Complaints of cyber-bullying are dealt with in accordance with our child protection procedures.

Contact details and privacy
As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian. Pupils are taught that sharing this information with others can be dangerous.

School and pupil websites – pictures and pupil input
As part of the IT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources. Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content. Pupils may design and create personal web pages, as part of the curriculum. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform. Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc. then identifying information will be removed, and images restricted.

Deliberate misuse of the Internet facilities
All pupils have discussed the rules for using the Internet safely and appropriately. These rules must be displayed in each classroom and the IT suite. Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

How will complaints regarding E-Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Due to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:
• All incidents will be recorded
• Interview/counselling by class teacher, Senior Leadership Team, Computing Lead, E-Safety Lead and Head teacher;
• Informing parents or carers;
• Removal/limiting of Internet or computer access for a period,
• Referral to LA / Police.

Our E-Safety Lead act as first point of contact for any complaint.

Class Rules for responsible IT use

Keep safe: Keep SMART

1. I will ask permission before using any IT equipment (e.g. computers, digital cameras, etc.), and only use it when a teacher or another adult is with me.

2. I will only use the school's computers for schoolwork and homework.

3. I will only delete my own files, and I will not look at other people's files without their permission.

4. I will use the usernames and passwords provided by the school to access the school network.

5. I will not bring software or USB memory sticks into school.

6. I will ask permission before using the Internet, and only use it when a staff member is present

7. I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use.

8. I will not use Google image search without being asked to do so by a school staff member.

9. I will not download anything (files, images etc.) from the Internet unless given permission.

10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail) at school.

11. The messages I send or information I upload as part of my school work will always be polite.

12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission.

13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member.

14. I will use the Kidsmart website to help me understand how to keep safe when using IT.

15. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe.

16. I understand that if I deliberately break these rules, my parents and the Head teacher will be informed.

Use of the Internet and IT resources by school staff

The Internet
Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.
We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability
To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

IT Equipment and Resources
The school also offers staff access to appropriate IT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use
Staff are expected to model appropriate IT and Internet use at all times. This supports our commitment to encouraging safe and appropriate IT and Internet use by our pupils both in school and at home. Staff are also careful to consider inclusion and equalities issues when using IT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies. Staff who need support or INSET in using IT as part of their professional practice can ask for support from the IT Lead.

Personal use of the Internet and IT resources
Some equipment (including laptops) is available for loan to staff, with permission from the Head teacher. The appropriate forms and agreements must be signed. However, all staff must be aware of the school policy on using school Internet and IT resources for personal use. These are outlined in the staff agreement form below.

E-mail
We recognise that e-mail is an essential tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups. Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this. E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, social media and forums, online chat and messaging
We realise that a growing number of educationalists and education groups use discussion groups, social media and online chat forums to share good practice and disseminate information and resources. The use of online discussion groups and social media relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages. The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements.

Data Protection (GDPR) and Copyright

The school has a Data Protection Policy in place as well as a Privacy Notice available in its website. These documents clearly outline why we hold data, how we obtain it, how we store it and when we destroy the data. – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and IT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary. Parent/carers have more control over the use of theirs and their child's data (including the use of their image). School MUST NOT SHARE IMAGES WITHOUT CONSENT.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

Data Protection Policy

Our school acts in accordance with the new GDPR Act which came in to force from May 2018. Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

Staff Laptop and IT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other IT equipment must adhere to all aspects of this E-Safety Policy. This must be the case wherever the laptop, computer or other such device is being used, as it remains the property of Red Hall Primary School at all times. Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense. Staff must sign the "Staff Laptop and Computer Loans Agreement" before taking the equipment away from the school premises

Red Hall Primary School

E-Safety Policy Staff Agreement Form

This document covers use of school digital technologies, networks etc. both in school and out of school.

Access

• I will obtain the appropriate log on details and passwords from the IT administrator.
• I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining the system.
• If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
• I will not allow unauthorised individuals to access school IT systems or resources.

Appropriate Use

• I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
• I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
• I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Computing Lead, E-Safety Lead or member of the SLT.

Professional Conduct

• I will not engage in any online activity that may compromise my professional responsibilities.
• I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
• I will never include pupils or former pupils as part of a non-professional social network or group.
• I will ensure that I represent the school in a professional and appropriate way when sending e- mail, contributing to online discussion or posting to public websites using school facilities.
• I will not browse, download or send material that could be considered offensive to colleagues
• I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.

Personal Use

• I understand that I may use Internet facilities for personal use at lunchtimes and break time, where computers are available and not being used for professional or educational purposes.
• I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
• I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' and similar material is forbidden.
• I will not use the school Internet facilities for personal access to public discussion groups or social networking sites.

Email

• I will only use the approved, secure email system for any school business.
• I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

Use of School equipment out of school

• I agree and accept that any computer or laptop loaned to me by the school, is provided mainly to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
• I will return school equipment regularly (to be agreed with IT Administrator) to be checked and updated.
• I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.

Teaching and Learning

• I will always actively supervise, or arrange for suitable supervision of pupils that I have directed or allowed to use the Internet.
• I will embed the school's E-Safety curriculum into my teaching, using agreed resources and materials.
• I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
• I will only use the Internet for professional purposes when pupils are present in an IT suite, or a classroom with Internet access.

Photographs and Video

• I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance).

Data protection

• I will not give out or share personal addresses (including email), telephone of any adult or students working at the school.
• I will not take pupil data, photographs or video from the school premises without the full permission of the Head teacher e.g. on a laptop, memory stick or any other removable media.
• I will ensure that I follow school data security protocols when using any confidential data at any location other than school premises.
• I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission.
• I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

Copyright

• I will not publish or distribute work that is protected by copyright.

• I will encourage pupils to reference online resources and websites when they use them in a report or publication

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent E-Safety policies. I agree to have a school user account, be connected to the Internet via the school network and be able to use the school's IT resources and systems.

Signature …… Date ……

Full Name .....(printed)

Job title ……

School ……

Authorised Signature (Head Teacher (primary) / Head/Deputy/ senior teacher (secondary) I approve this user to be set-up.

Signature …… Date……

Full Name .....(printed